CLAIMS

What is claimed is:

1. A method comprising:

establishing at least one cryptography service parameter threshold;

selectively detecting a request for at least one cryptography service; and

selectively performing at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold.

2. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying unacceptable cryptography algorithms.

3. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying acceptable cryptography algorithms.

4. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying at least one unacceptable cryptography key size parameter.

5. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying at least one acceptable cryptography key size parameter.

6. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier.

7. The method as recited in Claim 6, wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms.

8. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying at least one acceptable seed size parameter.

9. The method as recited in Claim 1, wherein establishing said at least one cryptography service parameter threshold includes at least identifying at least one unacceptable seed size parameter.

10. The method as recited in Claim 1, wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography system service, and another process calling into the cryptography application programming interfaces.

11. The method as recited in Claim 1, wherein selectively performing at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

12. The method as recited in Claim 11, wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold.

13. The method as recited in Claim 1, wherein selectively performing at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

14. The method as recited in Claim 13, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

15. The method as recited in Claim 1, wherein selectively performing at least one correctness detection action based on said requested cryptography service and said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, causing alteration of a graphical user interface, and forcing use of at least one other cryptography service.

16. A computer readable medium having computer-implementable instructions for causing one or more processing units to perform acts comprising:

selectively detecting a request for at least one cryptography service; and

selectively performing at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy at least one cryptography service parameter threshold.

17. The computer readable medium as recited in Claim 16, further comprising:

establishing said at least one cryptography service parameter threshold.

18. The computer readable medium as recited in Claim 17, wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts:

identifying unacceptable cryptography algorithms; and

identifying acceptable cryptography algorithms.

19. The computer readable medium as recited in Claim 17, wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts:

identifying at least one unacceptable cryptography key size parameter; and

identifying at least one acceptable cryptography key size parameter.

20. The computer readable medium as recited in Claim 17, wherein establishing said at least one cryptography service parameter threshold includes establishing a plurality of correctness categories, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier.

21. The computer readable medium as recited in Claim 20, wherein said plurality of correctness categories includes at least one correctness category selected from a group of correctness categories comprising authorized algorithms, unauthorized algorithms, weak algorithms, and strong algorithms.

22. The computer readable medium as recited in Claim 17, wherein establishing said at least one cryptography service parameter threshold includes at least one of the following acts:

identifying at least one acceptable seed size parameter; and

identifying at least one unacceptable seed size parameter.

23. The computer readable medium as recited in Claim 16, wherein selectively detecting said request for at least one cryptography service includes monitoring at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

24. The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

25. The computer readable medium as recited in Claim 24, wherein determining if said cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold includes comparing a size of said cryptographic key with said at least one cryptography service parameter threshold.

26. The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes determining if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

27. The computer readable medium as recited in Claim 26, wherein determining if said cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold further includes comparing a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

28. The computer readable medium as recited in Claim 16, wherein selectively performing said at least one correctness detection action based on said requested cryptography service if said requested cryptography service does not satisfy said at least one cryptography service parameter threshold includes performing at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, causing alteration of a graphical user interface, and forcing use of at least one other cryptography service.

29. An apparatus comprising:

cryptography correctness detection logic configured to selectively detect a request for at least one cryptography service, and selectively least one correctness detection action to be performed based on said requested cryptography service if said requested cryptography service does not satisfy at least one cryptography service parameter threshold.

30. The apparatus as recited in Claim 29, further comprising:

memory operatively coupled to said cryptography correctness detection logic; and

wherein said cryptography correctness detection logic is further configured to maintain said at least one cryptography service parameter threshold in said memory.

31. The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography algorithm, and at least one acceptable cryptography algorithm.

32. The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following: at least one unacceptable cryptography key size parameter; and at least one acceptable cryptography key size parameter.

33. The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to establish a plurality of correctness categories in said memory, wherein each at least one of said plurality of correctness categories includes at least one cryptography algorithm identifier.

34. The apparatus as recited in Claim 30, wherein said cryptography correctness detection logic is further configured to identify at least one of the following:

at least one acceptable seed size parameter; and

at least one unacceptable seed size parameter.

35. The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to monitor at least one process selected from a group of processes comprising an application, an operating system, a cryptography algorithm, and a cryptography application programming interface.

36. The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic key associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

37. The apparatus as recited in Claim 36, wherein said cryptography correctness detection logic is further configured to compare a size of said cryptographic key with said at least one cryptography service parameter threshold.

38. The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to determine if a cryptographic algorithm associated with said requested cryptography service is suitable for use based on said at least one cryptography service parameter threshold.

39. The apparatus as recited in Claim 38, wherein said cryptography correctness detection logic is further configured to compare a cryptography algorithm identifier with said at least one cryptography service parameter threshold.

40. The apparatus as recited in Claim 29, wherein said cryptography correctness detection logic is further configured to cause at least one action selected from a group of actions comprising interrupting at least one process, stopping at least one process, starting at least one process, displaying alert information, logging alert information, suggesting at least one alternative cryptography service, outputting alert messages, causing alteration of a graphical user interface, and forcing use of at least one other cryptography service, to be performed